TESTIMONY
OF
PROFESSOR JONATHAN TURLEY

J.B. and Maurice C. Shapiro Professor of Public Interest Law
George Washington University Law School

Before
Subcommittee on Intelligence, Information Sharing, and
Terrorism Risk Assessment

Committee on Homeland Security
United States House of Representatives

311 Cannon House Office Building

"*Protection of Privacy in the DHS Intelligence Enterprise*"

April 6, 2006

Chairman Simmons, Representative Lofgren, members of the Subcommittee, thank you for allowing me to appear today to testify on the important issues of privacy and homeland security.

I come to this subject with prior work as both an academic and a litigator in the areas of national security and constitutional law. As an academic, I have written extensively on electronic surveillance as well as constitutional and national security issues. I also teach constitutional law, constitutional criminal procedure and other subjects that relate to this area. As a litigator, I have handled a variety of national security cases, including espionage and terrorism cases. I am appearing today, however, in my academic capacity to address important issues related to domestic surveillance and homeland security.

I. GENERAL PRIVACY CONCERNS RAISED BY POST 9-11 SURVEILLANCE AND ENFORCEMENT.

The Department of Homeland Security (DHS) is the agency with the greatest ability to erode privacy since it has the dominant role, with the Federal Bureau of Investigation (FBI), in domestic enforcement activities.

Due to its size and diverse functions, the DHS has a much greater impact on privacy than any other agency. The DHS affects the lives of Americans to a far greater extent than most agencies because it has a far greater number of contacts with citizens in their everyday lives from airport security to disaster relief to immigration to customs. The DHS is not just a massive agency, it is a massive consumer of information from other agencies, state governments, private contractors, and private citizens. While the FBI is subject to criminal procedures and routine court tests, DHS is like a government iceberg with ninety percent of its work below the visible surface. This general lack of transparency makes it easier for abuses to occur by reducing the risk of public disclosure and review.

At risk is something that defines and distinguishes this country. Privacy is one of the touchstones of the American culture and jurisprudence. Indeed, it is a right that is the foundation for other rights that range from freedom of speech to freedom of association to freedom of religion. The very sanctity of a family depends on the guarantee of privacy and related protections from government interference.

Privacy is protected by the Constitution, including but not limited to the protections afforded by the Fourth Amendment. It is also protected in various statutes, such as the Privacy Act of 1974; E-Government Act of 2002, and the Federal Information Security Management Act of 2002 (FISMA). Further protections can be found in the substantive and procedural requirements of surveillance laws such as Title III and the Foreign Intelligence Surveillance Act (FISA).

Finally, there have long been practical protections of privacy. Until recent technological advances, there were practical barriers for the government to be able to conduct widespread surveillance on citizens. However, it is now possible to track citizens in real time with the use of advanced computers as recently made clear by the disturbing Terrorism Information Awareness (TIA) project of Defense Advanced Research Projects Agency (DARPA). These new technological advances constitute an unprecedented threat to privacy. Agencies like DHS often naturally gravitate to the accumulation of greater and greater information. Technology now allows these agencies to satiate that desire to a degree that would have been unthinkable only a couple of decades ago.

Despite these protections, privacy remains the most fragile and perishable of our fundamental rights. When pitted against claims of national security, privacy is often treated as an abstraction and government officials offer little more than rhetorical acknowledgement of privacy concerns in their programs and policies. The resulting uncertainty is the very scourge of privacy. Privacy depends on a certain expectation of citizens that they are not being watched or intercepted. When uncertain of the government's commitment to privacy or legal process, citizens often experience a chilling effect that inhibits the exercise of free speech and other rights.

The uncertainty over privacy is clear in recent polls and studies. Notably, the DHS receives one of the lowest scores on the privacy question. The 2006 Privacy Trust Study of the Ponemon Institute gave the DHS only a 17 percent score, down by 10 percent from the previous year.

This freefall is more than a public relations problem. Our constitutional test for privacy under the Fourth Amendment is based on "the reasonable expectation of privacy" under the *Katz* doctrine. To the extent that a citizen has a reasonable expectation of privacy, the government is usually required to satisfy a higher burden, including the use of a warrant for searches. The *Katz* test has now created a certain perverse incentive for government. As agencies like DHS reduce that expectation of privacy in the public, it actually increases the ability of the government to act without protections like warrants. The result is a downward spiral as reduced expectations of privacy lead to increased government authority which lead to further reduced expectations.

Privacy concerns after 9-11 have grown with each year in the war on terror. There is a pervasive view that the Administration is wielding unchecked and, in some cases, unlawful authority in the war on terror. In areas that range from enemy combatant detentions to warrantless domestic surveillance programs to data mining of private records, the chilling effect for privacy and civil liberties has become positively glacial for many citizens, particularly citizens of the Muslim faith or Middle Eastern descent.

Just in the last few months, Congress has faced a remarkably wide range of issues that directly threaten privacy rights and civil liberties. It is regrettably a long and lengthening list. Today, in the interests of time, I wanted to focus on a few of the most recent controversies to show how privacy rights and civil liberties are eroded by the aggregation of otherwise

disparate and insular programs. While these examples may appear unrelated, they each impact privacy rights and civil liberties in significant ways. The point that I wish to convey is that privacy is being undermined in a myriad of ways and that any effort to protect this right will have to be equally comprehensive.

a. **The Failure to Comply with Privacy Standards, including the Use of Reseller Information That Lack Fair Information Practices.** As shown recently by the GAO, the DHS is using an increasing amount of data from information resellers that lack critical protections and fair information practices. The recent misuse of 100 million personal records in alleged violation of the Privacy Act typifies this concern.

b. **Over-classification and Reclassification Efforts**. The Administration has led a serious rollback in the efforts to gain greater transparency in government by over-classifying and reclassifying basic documents and information. Agencies like DHS can prevent disclosure of misconduct or negligence by using classification rules to avoid review.

c. **Registered Traveler Programs**. The DHS continues to encourage the creation of registered traveler programs that would assemble a databank of pre-screened passengers. Whether run privately or governmentally, these programs offer illusory security but present serious threats to civil liberties.

d. **Failure to inform Congress of Surveillance Programs like the NSA operation**. One of the greatest protections of civil liberties is the separation of powers doctrine and its inherent system of checks and balances. The failure to inform the members of Congress, particularly the full committee membership of the intelligence committee, of ongoing intelligence activities negates any meaningful oversight functions.

e. **New Threats Against Whistleblowers**. Legislation to increase penalties for federal whistleblowers is a startling reaction to the disclosure of unlawful activity. This is exemplified by the proposed increase in penalties for officials seeking to disclose unlawful activity under the NSA domestic surveillance program. Likewise, the continued refusal of Congress to pass a federal shield law for

journalists can only be seen as an intentional deterrent for whistleblowers. When an official at DHS is aware of an unlawful program, the media may be the only effective way to stop the illegality.

These are a few of the most recent examples of how privacy rights and civil liberties protections are being pummeled across a long spectrum of insular governmental policies and programs. If Congress truly wants to protect privacy, it must deter threats by increasing both the likelihood of disclosure of unlawful conduct and the penalties for such conduct. This requires greater transparency in agencies like the DHS, better oversight in Congress, and fuller protection for those who seek to disclose misconduct.

II. THE NSA DOMESTIC SURVEILLANCE PROGRAM

The recent NSA operation brings together many of the most dangerous elements discussed above: lack of congressional oversight, the violation of federal law, the pursuit of whistleblowers, and finally the absence of any meaningful action from Congress. In terms of privacy rights, the NSA operation also presents the most serious attack on the guarantees that are essential for the exercise of the full panoply of rights in the United States.

The disclosure of the National Security Agency's (NSA) domestic spying operation on December 16, 2005 has created a constitutional crisis of immense proportions for our country. Once a few threshold, and frankly meritless arguments of legality are stripped away, we are left with a claim of presidential authority to violate or circumvent federal law whenever a president deems it to be in the nation's security interests. As I made clear in a January hearing, these claims lack any limiting principle in a system based on shared and limited government. It is antithetical to the very premise of our constitutional system and values.

This is, of course, not the first time that President Bush or his advisers have claimed presidential authority to trump federal law. In its infamous August 1, 2002 "Torture Memo," the Justice Department wrote that President Bush's declaration of a war on terrorism could "render moot federal law barring torture." The Justice Department argued that the enforcement of a statute against the President's wishes on torture "would

represent an unconstitutional infringement of the president's authority to conduct war."

The President also assumed unlimited powers in his enemy combatant policy, where he claimed the right to unilaterally strip a citizen of his constitutional rights (including his access to counsel and the courts) and hold him indefinitely.

On December 30, 2005, President Bush again claimed authority to trump federal law in signing Title X of the FY 2006 Department of Defense Appropriations Act. That bill included language outlawing "cruel, inhumane or degrading treatment" of detainees, such as "waterboarding", the pouring of water over the face of a bound prisoner to induce a choking or drowning reflex. In a signing statement, President Bush reserved the right to violate the federal law when he considered it to be in the nation's interest.

The NSA operation, however, is far more serious because the President is claiming not just the authority to engage in surveillance directly prohibited under federal law, but to do so domestically where constitutional protections are most stringent. The scope of this claimed authority is candidly explained in the Attorney General's recent whitepaper, "Legal Authorities Supporting the Activities of the National Security Agency Described by the President." As I noted in the prior hearing, it is a document remarkable not only in its sweeping claims of authority but its conspicuous lack of legal authority to support those claims. It is also remarkably close to the arguments contained in the discredited Torture Memo.

The vast majority of experts in this field have concluded that the NSA program is unlawful. Even stalwart Republican members and commentators have rejected its legality. It is an inescapable conclusion. Under Section 1809, FISA states that it is only unlawful to conduct "electronic surveillance under color of law except as authorized by statute." The court in *United States v. Andonian*, 735 F.Supp. 1469 (C.D. Cal. 1990), noted that Congress enacted FISA to "sew up the perceived loopholes through which the President had been able to avoid the warrant requirement."

FISA does allow for exceptions to be utilized in exigent or emergency situations. Under Section 1802, the Attorney General may authorize warrantless surveillance for a year with a certification that the interception is exclusively between foreign powers or entirely on foreign property and that

"there is no substantial likelihood that the surveillance will acquire the contents of any communications to which a United States person is a party."

No such certification is known to have occurred in this operation. Nor was there an authorization under Section 1805(f) for warrantless surveillance up to 72 hours under emergency conditions. Finally, there was no claim of conducting warrantless surveillance for 15 calendar days after a declaration of war, under Section 1811.

The NSA operation was never approved by Congress. Moreover, the Administration's attempts to use the Authorization for Use of Military Force, Pub. L. 107-40, 115 Stat. 224 (2001), as such authorization is beyond incredible, it is unfathomable. With no exceptions under the Act, the NSA operation clearly conducted interceptions covered by the Act without securing legal authority in violation of Section 1809.

The NSA operation is based on a federal crime ordered by the President not once but at least 30 times. Indeed, in his latest State of the Union Address, President Bush pledged to continue to order this unlawful surveillance. A violation of Section 1809 is "punishable by a fine of not more than $10,000 or imprisonment for not more than five years, or both." Likewise, an institutional defendant can face even larger fines and, under Section 1810, citizens can sue officials civilly with daily damages for such operations.

The DHS is likely a recipient – directly or indirectly – of the information gathered under this unlawful program. In my view, government officials participating in this program are participating in an ongoing criminal enterprise. The DHS officials have an independent obligation to determine if this program is lawful and to refuse to participate on any level with the program if it is viewed as unlawful. This includes the receipt or use of intelligence. Moreover, to the extent that federal courts determine that this operation is unlawful, the incorporation of the intelligence in DHS investigations or enforcement may ultimately result in undermining those activities. Under a classic "fruit of the poisonous tree" theory, the use of this tainted intelligence can taint any information gathered as a result of its use.

Putting aside the questions of criminality, the NSA operation jeopardizes basic privacy guarantees. First, it shows an unchecked and

unilateral exercise of presidential authority. Second, the conspicuous absence of congressional oversight has destroyed any faith in a legislative check on such authority. Finally, it created uncertainty for citizens as to their guarantees of privacy and civil liberties under this program or other undisclosed programs.

III. WHAT CAN BE DONE?

Just as there are a myriad of threats to privacy, there are a myriad of possible measures to protect privacy interests. The most significant protections often come in the form of protecting those who would reveal violations while deterring those who would commit the violations. Such reforms include the following:

a. Investigation of the NSA domestic surveillance program with public hearings.

b. Strengthening of whistleblower protections, particularly for employees at defense, intelligence, and homeland security agencies.

c. Strengthening laws on data mining and data sharing by agencies, including meaningful deterrents for agencies like DHS that violate the Privacy Act and other statutory protections.

d. Reverse the trend toward reclassification and over-classification of documents that decreases the transparency of government by enacting new avenues to challenges overbroad assertions of classified status.

e. The Congress should prohibit not simply a government-run registered traveler system but a private-run system. The DHS support for a pilot program in Orlando should be ended by barring the expenditure of any federal funds and prohibiting the incorporation of such a program into TSA airport security systems.

f. Congress should require compliance with conferral rules on all intelligence operations (other than covert activities) so that all

members of the intelligence committees are informed of operations like NSA's domestic surveillance program.

g. A new system of privacy officers should be established so that every major office in agencies like DHS have a privacy officer who will be responsible for training, enforcing, and certifying compliance with federal privacy laws.

h. Enhancing the authority and funding for the DHS Privacy Officer. While Congress created this position in the Homeland Security Act of 2002, there is a widespread view that the privacy officer needs greater authority and access as well as more resources to police the programs of this massive agency. The slow response of the DHS to establish this office indicates a lack of internal support of the model of an independent internal watchdog office. For this reason, changes should include a reporting requirement not only to the DHS but directly to Congress.

i. Congress should pass a federal shield law for journalists, as has virtually every state. Increasing legal threats for journalists, including contempt rulings, presents an obvious deterrent to any whistleblower seeking to disclose unlawful conduct.

j. Congress should require an annual report, with regular public hearings, on privacy matters to identify emerging threats to privacy and possible legislative solutions.

IV. CONCLUSION

These threats to privacy rights and civil liberties have created not just a constitutional crisis but a test for every citizen. Our legal legacy was secured at great cost but it can be lost by the simple failure to act. The President is right: these are dangerous times for our constitutional system. However, it is often the case that our greatest threats come from within. Indeed, Justice Brandeis warned the nation to remain alert to the encroachments of men of zeal in such times:

> Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasions of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachments by men of zeal, well-meaning but without understanding.

Citizens, let alone congressional members, cannot engage in the dangerous delusion that they can remain silent and thus remain uncommitted in this crisis. Remaining silent is a choice; it is a choice that will be weighed not just by politics but by history.

Thank you for the opportunity to speak with you today and I would be happy to answer any questions that you might have at this time.

Jonathan Turley
Shapiro Professor of Public Interest Law
George Washington University Law School
Washington, D.C. 20052
(202) 994-7001
jturley@law.gwu.edu